Transactions on Engineering and Computer Science

Research| Vol 2 Iss 1

Cybersecurity Risk Management Plan for a Blockchain Application Model

Gabriel Kabanda*

Zimbabwe Academy of Sciences, TREP Building, University of Zimbabwe, Zimbabwe

***Corresponding author:** Kabanda G, Zimbabwe Academy of Sciences, TREP Building, University of Zimbabwe, Zimbabwe; +263-712-452795; E-mail: gabrielkabanda[AT]gmail[DOT]com

Received: February 11, 2021; **Accepted:** March 23, 2021; **Published:** April 05, 2021

Abstract

The substantive increase in the use of internet-based technologies has subjected organizations to malicious attacks. Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. A blockchain is a datastructure, which stores transactional records in the form a block chained and stored in several databases, and is fundamentally a digital ledger of transactions (DLT) that upon duplication is distributed on the blockchain throughout the entire computer network. To improve on Cybersecurity, Machine Learning is considered for data mining among the data. This research is purposed to determine a cybsersecurity risk management plan, develop a Blockchain Technology Application Model that manages cyber risks and vulnerabilities, ascertain how the Framework of Blockchain Technology and Cryptocurrency addresses cyber risks and creates value to the financial services sector. The research used the Pragmatism paradigm, which is a philosophy that is closely linked to the Mixed Method Research (MMR). The Focus Group comprised a total of 100 participants from the Masters students attending the Applied Business Informatics module taught by the author at the University of Zimbabwe in 2020. The National Institute of Standards and Technology (NIST) Cybersecurity Framework and the General deterrence theory (GDT) were used to formulate the Cybersecurity strategy. Blockchain cyber vulnerabilities were determined. A model structure for block chain technology and cryptocurrency was developed and an explanation provided on how the framework of Blockchain Technology and Cryptocurrency addresses cyber risks and creates value to financial services sector.

Keywords: ***Cybersecurity; Artificial Intelligence; Machine Learning; Cyber Risk; Blockchain Technology; Cryptocurrency; Bitcoins; Pragmatism paradigm.***

Citation: Kabanda G. Cybersecurity risk management plan for a blockchain application model. Trans Eng Comput Sci. 2021;2(1):121.

1. Introduction

1.1 Background

Cybersecurity is the practice of protecting systems, networks, and programs from digital (malicious) attacks. Cyberattacks can potentially target access, change or destroy sensitive information; can be used to extort money from people; or disrupt normal business operations. Cybersecurity is the policy framework and technologies purposed to protect the confidentiality, assurance, and availability of computing resources from attack [4]. [12] also states that cyber security entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption. The currrent trends in Cybersecurity in 2021 includes the following:

- Phishing and Social Engineering (Phishing is the practice of sending fraudulent emails that resemble emails from reputable sources.)
- Ransonware (Ransomware is a type of malicious software. It is designed to extort money by blocking access to files or the computer system until the ransom is paid)
- Internet of Things (IoT) Susceptibility (The Internet of things (IoT) is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction)
- Cloud Vulnerability and Cloud Security (Microsoft Azure, Google Cloud Platform (GCP), Amazon (AWS)).
- Third-party vulnerabilities
- Internal attacks
- Data Rights Compliance

Sensors, analyzers and a user interface constitute a network intrusion detection and prevention system, as shown on Fig. 1 below, depicted as Intrusion Detection System (IDS) components.

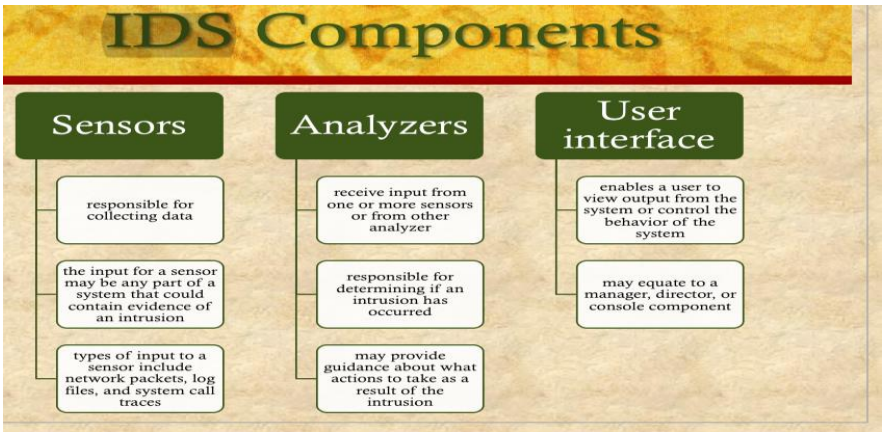


Fig. 1. The IDS components (Source: [18]).

New technologies often come with new security concerns. According to [6], research in network anomaly detection has applied several well-known Artificial Intelligence paradigms to address the security concerns.

"Cybersecurity Risk Management" means policy frameworks and technologies that thwart risks in computer networks, applications and data in a networked environment and its associated assurance.

The common types of attacks in using the Internet of Things (IoT) identified by [8] are tabulated below on Table 1. A denial of service (DoS) attack renders a system inaccessible by its legitimate users.

Table 1: Layer-Based Attacks in IIoT systems (Source: [8]).

Layer	Attacks	Description
Application	Injection	Untrusted data that is sent to an interpreter or database
	Brute force	An attempt to guess a password via sending various passwords
	Malware	A malicious code can attack mail and web services
Middleware	Flooding	Repeating the request of a new connection until the IIoT system reaches maximum level.
	De-synchronization	Disruption of an existing connection
Network	DoS	Attempt to stop or reduce activity of an IIoT
	MIM	Violating data confidentiality or integrity during transfer
	HELLO flood	Uses HELLO packets as weapon to launch the attack on IIoT system
	Sybil	A single node duplicates its node to be in multiple locations
Perception	Eavesdropping	Deducing data sent by IIoT devices across network
	RFID tracking	Modifying a content of a tag or trying to disable it
	Jamming	Creating radio interference and exhaustion on IIoT devices

One of the latest IT solutions that require information security risk management (ISRM) and considered not only as an innovative technology, but as a potential revolution in the business is Blockchain. Risk analysis includes processes such as identification of activity, threat analysis, vulnerability analysis and guarantees. One of the completed phases in information security risk assessment process is risk analysis.

A blockchain is a datastructure, which stores transactional records in the form a block chained and stored in several databases, and is is fundamentally a digital ledger of transactions (DLT) that upon duplication is distributed on the blockchain throughout the entire computer network. Blockchain is a type of DLT where a hash is used to record the transactions with an immutable cryptographic signature. A group of transactions constitute a block, and a record of every transaction is appended to every participant's ledger. The basic process of Blockchain is shown on Fig. 2 below.

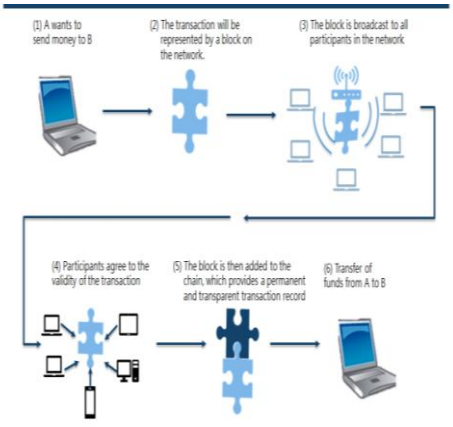


Fig. 2. Basic process of blockchain.

A cryptocurrency is a digital currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Many cryptocurrencies are decentralized networks based on blockchain technology. The purpose is to enable micro-transactions at a very low cost [25]. One of the most commonly used application of blockchain technology is Cryptocurrency.

The National Institute of Standards and Technology (NIST) emphasizes that blockchain technology:

- Groups the signed transactions according to a certain cryptographic pattern into blocks that form a ledger.
- Secures the ledger by a cryptographic link to each block and its validated previous entry.
- Automatically manages conflicts using established rules.
- Duplicates the ledger copies across the entire network.

Blockchain mainly relies on three concepts which are:

- Peer-to-peer network
- Distributed Consensus
- Public-key Cryptography.

The basic benefits of using Blockchain Technology include the following:

- Time savings
- Cost savings
- Tighter security
- Enhanced privacy
- Improved auditability
- Increased operational efficiency

Artificial Intelligence (AI) is about computer systems that simulate human intelligence processes, including learning, reasoning, and self-correction. AI works with the help of Artificial Neurons (Artificial Neural Network) and scientific theorems (If-Then Statements, Logics). The special ability of AI is to reach a solution based on facts rather than on a preset series of steps, and this is what most closely resembles the thinking function of the human brain. AI is characterised by the ability to simulate human behavior and cognitive processes, capture and preserve human expertise, obtain fast response, and manage huge volumes of data quickly. On the contrary, human intelligence is about intuition, judgement, common sense, creativity, beliefs, effective communication, plausible reasoning and critical thinking.

Machine Learning (ML) is the enabling process of computers to learn. ML is regarded as a scientific discipline concerned with the design and development of algorithms that allow machines to mimic human intelligence. Artificial Neural Networks (ANNs) are the ML algorithms inspired by the central nervous system, where computers are programmed to teach themselves from data as opposed to instruction to perform specific tasks. ML can handle data mining among the data. [20] classified ML into three classes:

- Supervised learning
- Unsupervised learning, and
- Reinforcement learning.

The roadmap for building a Machine Learning System is shown on Fig. 3 below.

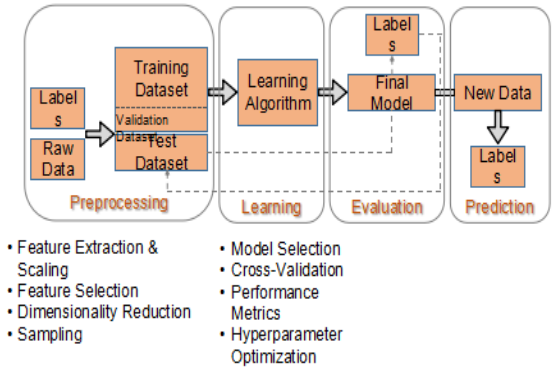


Fig. 3. Roadmap for building machine learning systems.

1.2 Statement of the problem

The substantive increase in the use of internet-based technologies has subjected organizations to malicious attacks. A blockchain is a datastructure, which stores transactional records in the form a block chained and stored in several databases, and is fundamentally a digital ledger of transactions (DLT) that upon duplication is distributed on the blockchain throughout the entire computer network. To improve on Cybersecurity, ML is considered in order to do data mining among the data.

There is need for proactive security measures against cyber attacks, and in particular a cybsersecurity risk management plan which leads to the development of a Blockchain Technology Application Model that manages cyber risks. It is of primordial importanve to ascertain how the Framework of Blockchain Technology and Cryptocurrency addresses cyber risks and creates value to the Financial Services sector.

1.3. Research Objectives

The major objectives of this research were to:

- Determine the cybersecurity risk management plan that incorporates Machine Learning (ML) algorithms.
- Develop a Blockchain Technology Application Model that manages cyber risks and vulnerabilities.
- Ascertain how the Framework of Blockchain Technology and Cryptocurrency addresses cyber risks and creates value to the Financial Services sector.

1.4. Research Questions

The key research questions were as follows:

- What is the proactive cybersecurity risk management plan that incorporates Machine Learning algorithms?

- How do you develop a Blockchain Technology Application Model that manages cyber risks and vulnerabilities?
- How does the Framework of Blockchain Technology and Cryptocurrency address cyber rsisks and creates value for the Financial Services sector?

2. Literature Review

According to National Institute of Standards and Technology (NIST) [15], the NIST Cybersecurity framework is purposed to reduce cyber risk and improve security to the critical infrastructure. The NIST Cybersecurity Framework shown on Fig. 4 provides organizations with a mechanism to:

- depict the current cybersecurity state
- represent describe the proper cybersecurity condition
- identify and prioritize improvement opportunities
- progressively move towards the desired cybersecurity state
- communicate the cybersecurity risk with all the key stakeholders.

The NIST framework [15] comprises five elements which are purposed to identify, protect, detect, respond and recover the network in the unlikely event of a cyber-attack, as shown below on Fig. 4.

Fig. 4. NIST Cybersecurity framework core components. (Source: [15]).

The General Deterrence Theory advocates the use of strong deterrents and penalties to dissuade people from doing malpractices and perpetrating cyber-attacks [21]. The four main elements of the General Deterrence Theory are illustrated in Fig. 5 below [2]. The whole interaction process among the attacker and the protecting agent can be presented as a Game theory approach that could serve as a balancing and strategizing tool for predicting the behavior of the attacker and based on the solution to that game, to find an equilibrium point for optimal results.

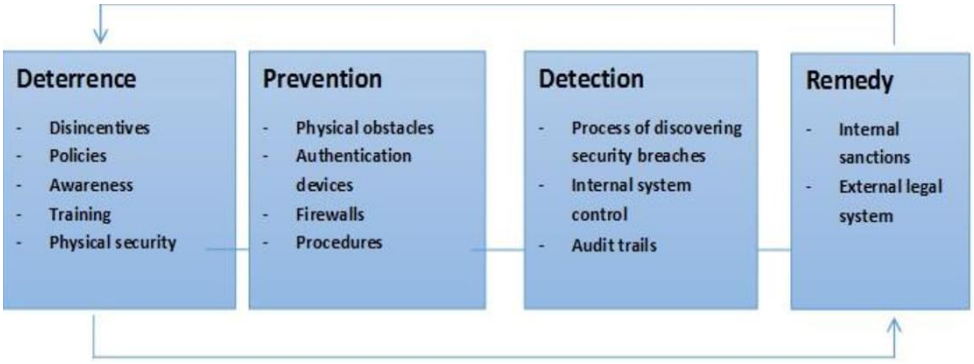


Fig. 5. Elements of the General Deterrence Theory (GDT) (Source: [2]).

Cryptography encrypts the information into an unreadable, referred to as cipher text, in order to protect the information. The recipient, who possesses a secret key, is the only one who can decipher it into plain text. Data is valuable and needs to be protected. Cryptographic algorithms can be classified in various ways, but the major focus is on the number of keys that are employed for encryption and decryption, and by their use. The three types of algorithms that are commonly used are [22][1].

- *Secret Key Cryptography (SKC):* Primarily used for privacy and confidentiality, uses a single key commonly referred to as the **symmetric encryption**.
- *Public Key Cryptography (PKC):* Uses one key for encryption and another for decryption; also called **asymmetric encryption,** and this primarily used for authentication, non-repudiation, and key exchange.
- *Hash Functions:* These are primarily used for message integrity and uses a mathematical transformation to irreversibly "encrypt" information using a digital fingerprint.

The training phase in NIDS is represented by Fig. 6 below, which shows the importance of the algorithm used and the data for training in order to develop a final method after a refinement process through a refiner model.

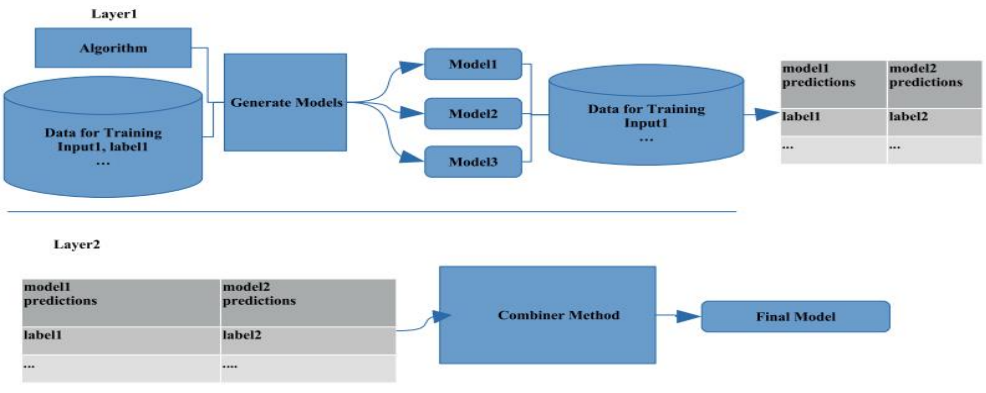


Fig. 6. Training phase of tracking approach (Source: [7]).

[1][Online]. Available: https://www.garykessler.net/library/crypto.html

2.1 Bitcoins and cryptocurrency

The brief history of Bitcoins is shown on Fig. 7 below.

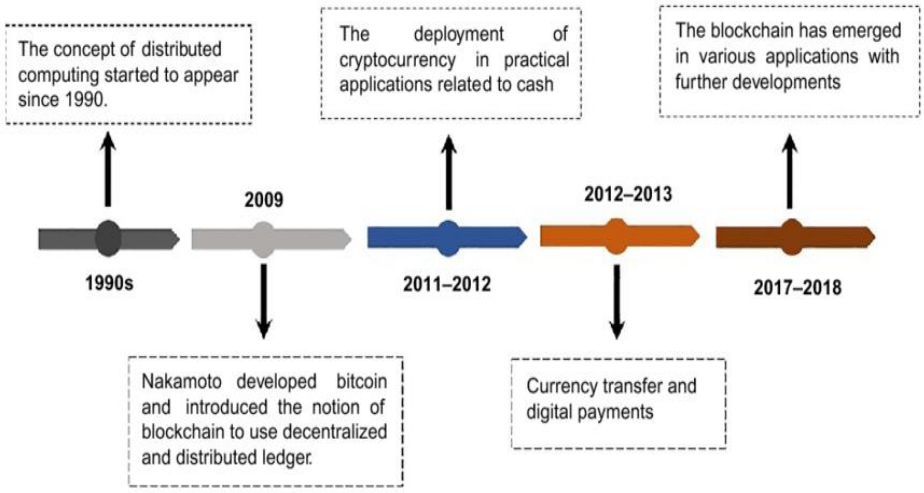


Fig. 7. History of bitcoins (Source: Adopted from [3]).

2.1.1 Anonymity of bitcoins

One of the advantages of using bitcoins is anonymity, as was highlighted by [12] and [5]. Anonymity is unique and not shared publicly [12]. Transactions are irreversible in the bitcoin network and it is close to impossible to trace back a transaction.

2.1.2 Volatility of bitcoins

The volatility of cryptocurrencies arise from the fact that there is no central authority regulating them and their supply is fixed. There is no policy in place to regulate the growth in cryptocurrencies such as the monetary policy in fiat currencies. So, since bitcoins have no central bank to regulate inflation, the currency has become an instrument of speculations.

2.1.3 Lack of adequate infrastructure

The lack of adequate information communications technology (ICT) infrastructure in most developing nations present challenges for the adoption of crypto currencies in countries like Zimbabwe as these require internet connection for their trading and movement. However, ICT development in sub-Saharan Africa has grown rapidly the past decade. According to [9] the overall mobile subscription penetration in Africa reached 44% in 2017 compared to 25% from 2010. The growing access to mobile connectivity has been vital to empower people and driving economic growth by increasing efficiency and productivity. The same report by [9] also suggests that Mobile adoption has also had its impact on labor, estimated to have created 3 million jobs in 2017. The same report states that 7.1% of the GDP ($110 billion) across sub-Saharan Africa is generated by mobile technologies and services and is projected to constitute 7.9% of GDP ($150 billion) by 2022 [9]. Even though it is getting more common for people in urban areas to have a mobile phone, the mobile coverage is still limited in rural areas with an absence of fixed connectivity, electricity grids and consequently an internet connection [23].

2.2 Benefits of Blockchain Technology

The benefits of using blockchain technology in digital currency includes the following:

2.2.1 Decentralization

To reduce the cyber-crime storage risks, a decentralized fashion is used to store the customer records and encourage consistency in the recording processes.

2.2.2 Improved Privacy Control

A single trusted third party can no longer adequately handle customer information. Smart contracts can be used to handle customers' data on behalf of the entire financial ecosystem.

2.2.3 Immutability

Customer information recorded in the blockchain is permanent and cannot be changed, which is crucial for tracking as the information is easily accessible by all financial institutions involved.

2.2.4 Customer Product Personalization and Profile Management

Block chain technologies can enable much more accurate, secure and privacy friendly profiling of both consumers and businesses, which accommodates personalized customer profiles.

2.3 Information risk management process

The Information Risk Management Process is illustrated on Fig. 8 shown below.

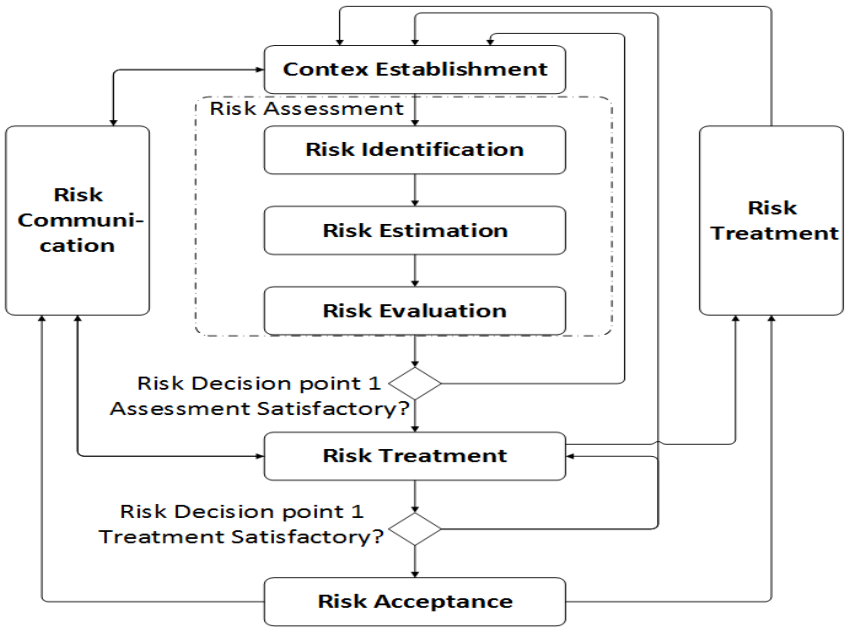


Fig. 8. The ISO/IEC 27005: 2011 information security risk management process (Source: [1]).

3. Research Methodology

The research used the Pragmatism paradigm, which is a philosophy that is closely linked to the Mixed Method Research (MMR). Pragmatism places a greater emphasis on practical solutions to applied research questions and inquiry, and prefers those methods and theories which are practical and more useful for use in specific contexts [17]. Pragmatism mixes both qualitative and quantitative methods on the basis of "what works".

In this research, a mixed method approach was taken, which involves mixing both qualitative (Focus Group discussions) and quantitative methods (an experiment). Literature review and document analysis were also used in this research.

The Focus Group comprised a total of 100 participants from the Masters students attending the Applied Business Informatics module taught by the author at the University of Zimbabwe in 2020.

4. Results and Analysis

4.1 Cybersecurity national challenges

The national challenges of Cybersecurity as given by the Focus Group includes the following:

- Lack of clarity on the responsibilities with regards to ownership of Cybersecurity roles.
- The monotonic increase in the ubiquitous nature of technology and raid advances in the Internet of Things (IoT), which increases the risk on cybersecurity.
- The exclusion of Cybersecurity strategy in the formulation and development of the Business Strategy of organizations.
- The risk of over relience on one service provider to effect financial transactions at a national level.
- Inadequate enforcement of Service Level Agreements (SLAs) with service providers to ensure performance.
- Low internet penetration rates for the majority of the people in smaller towns, villages and other remote areas.
- Lack of adequate technical measures to handle Cybersecurity.
- Inadequate national awareness training programmes and campaigns.
- Huge skills gaps in Cybersecurity and delinquency in the competence levels.
- There is no simplification of the national ICT Policies and Cybersecurity policies for the benefit of ordinary citizens and people at grassroots levels.
- The higher education system is not offering meaningful programmes and courses on Cybersecurity skills and competences.

4.2 Cybersecurity framework

The Cybersecurity Framework in developing nations faces the challenges in infrastructure, legal frameworks, educational awareness campaigns, Cybersecurity skills gaps, affordability by the majority of the population, and inappropriate frameworks.

The procedures for managing information security issues can be spelt out in organizational policies [16]. However, a complete Cybersecurity vision is required in each case.

4.3 Risk Management Process

The Cybersecurity risk management plan includes:

- Risk Analysis;
- Risk Assessment;
- Risk Mitigation;
- Risk Monitoring

The Risk Management process is illustrated in Fig. 9 below.

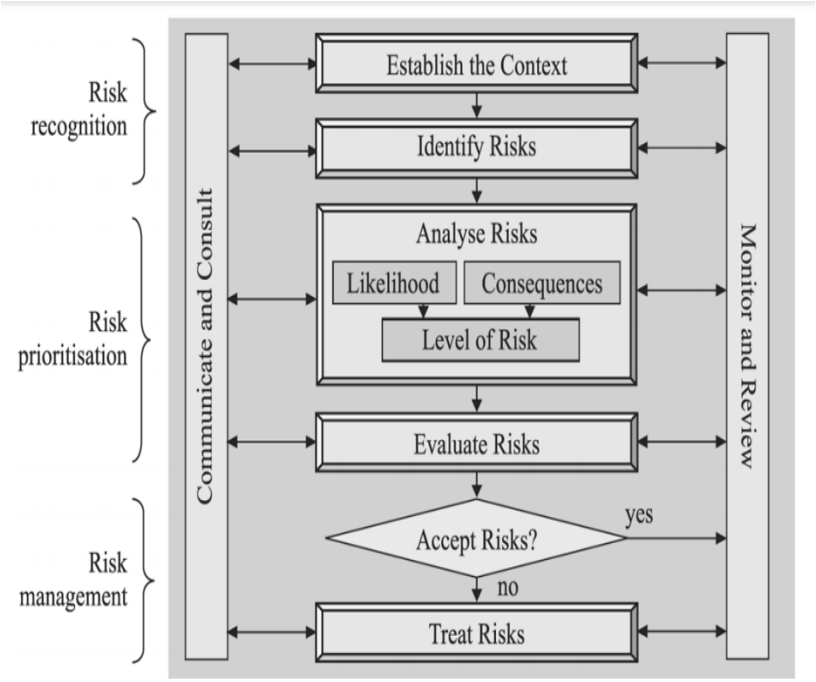


Fig. 9. Risk management process.

The elements of the Cybersecurity Risk Management Plan include the following:

- NIST Cybersecurity Framework with a focus on Identify, Protect, Detect, Respond, Recover dimensions
- Risk Types (focus on 6 risk types) which are Technology, Information, Cyber Risk, Business Resilience, Reputational and Regulatory Risk
- Governance Risk & Compliance
- Third Party Risk Management
- Policies, Standards and Procedures
- Risk Assessment (Identify, Assess, Develop Controls & Make Decisions, Implement Controls, Supervise and Evaluate).

4.4 Blockchain cyber vulnerabilities

The Blockchan cyber vulnerabilities identified were as follows:

- *Blockchain code vulnerabilities* from applications that may have inherent software coding errors or have high dependence on encryption algorithms [26].
- *Blockchain platform vulnerabilities from* applications that run on general purpose operating systems and platforms with known risks.
- *End-User vulnerabilities, e.g. hacking of online wallets, theft of a private key, etc.*
- *Wallet controls as* digital wallet providers are now minimizing individuals risks and providing better key management services, but the risk is still high on the use of passwords and other user authentication controls [1].

4.5 Model structure for blockchain technology and cryptocurrency

The model structure for Blockchain Technology developed is shown on Fig. 10 below.

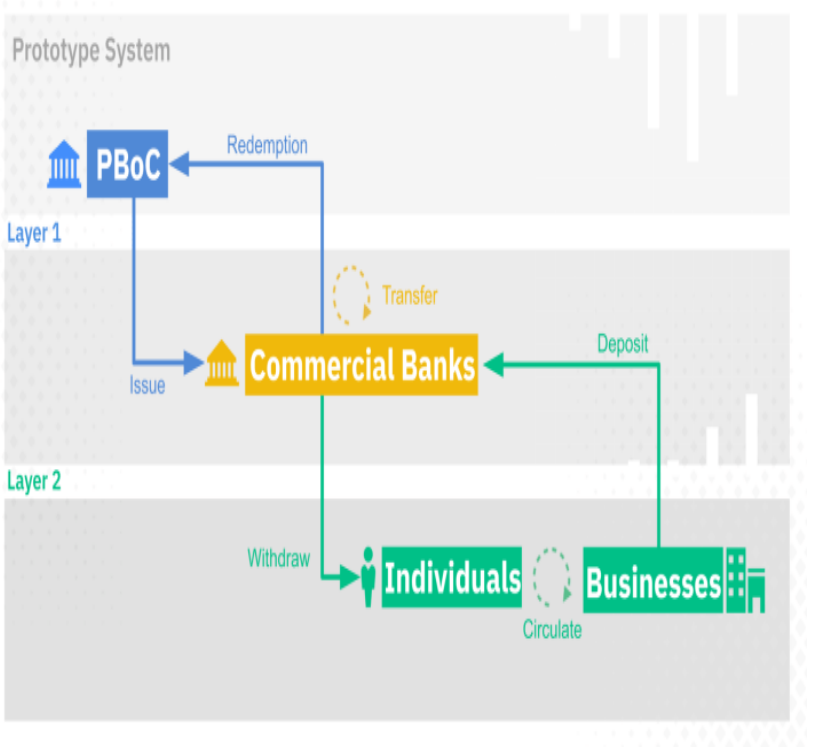


Fig. 10. Model structure for blockchain technology and cryptocurrency.

The five major components of the model structure are:

- The Distributed Ledger Technology Cryptographic hash functions
- The DLT Public-Private Key Cryptography
- The DLT Nodes
- The DLT Tokens
- The DLT Blocks in a blockchain to record transactions.

4.6 Central Bank Digital Currency (CBDC)

Central Bank Digital Currency is commonly defined as the value of digital representation, electronic storage, and cryptographic transfer, that is expressed digitally, stored electronically, and encrypted for transfer of ownership. It is issued and managed by a sovereign institution such as the Central Bank, subject to the financial laws and regulations in that country. Thus, a Central Bank Digital Currency (CBDC) is a form of centralised cryptocurrency, or another form of fiat money, similar to coin and banknote. The functions of CBDC includes the following:

- Centralized issuance: implies that it is backed by central banks. The monetary policy is formulated by the central bank, such that CBDC has the intrinsic value.
- Transferability: implies that CBDC can be used as a means of circulation and payment for ongoing value movements in economic activities. The CBDC also needs to achieve the split maintaining the zero-sum principle for more efficient and convenient circulation.
- Storability: CBDC and the transaction history are securely stored in the form of electronic data in an organization or user's electronic device for query, payment, exchange and management.
- Offline transaction: Offline transaction of CBDC specifically means that it may not directly communicate with the host servers or the main system when the transaction is performed through the electronic device, and the payer does not exchange information with other devices or systems through communication methods such as wired or wireless.
- Exchangeability: In the circulation of CBDC in the digital world, it is also necessary to satisfy the exchangeability, including the equivalent exchange between one CBDC and other forms of the same sovereign currency, as well as the foreign exchange between CBDC and other sovereign currency.

The three-layered blockchain and cryptocurrency application technology model are as follows.

- *Regulatory Layer:* The regulatory layer is mainly in charge of controlling and governing the whole life cycle of CBDC throughout the technical and policy aspects, so as to maintain the healthy and stability of the financial environment dominated by CBDC. The Regulatory layer mainly includes the Central Bank, public key infrastructure (PKI) with identity authentication as the core, and other regulatory bodies such as sovereign institutions.
- *Network Layer:*The network layer is a bridge between the top regulators and ordinary users. It is different from the p2p network structure mostly adopted by decentralized cryptocurrencies, network layer in CBDC adopts two different network structures. One is a tree hierarchy structure centred on central bank and other regulatory agencies, and the other is a local distributed structure composed of commercial banks and other third-party operators.
- *User Layer*: User layer comprises the low-level users and their transactions, which are not only the regulatory objects of regulatory player, but also the main data source for verification and processing of network layer. User layer contains cash exchange, CBDC deposit, and CBDC withdrawal, inter-bank payment, cross bank payment, cross-border payment and currency exchange.

4.7 An Explanation on how the framework of blockchain technology and cryptocurrency addresses cyber risks and creates value to the financial services Sector

The fully enunciated explanation of how the framework of Blockchain Technology and Cryptocurrency addresses cyber risks and creates value to the financial services sector is as follows:

- *Minimal Transaction Fees:* Because cryptocurrency transfers are peer-to-peer and require no centralized intermediaries, transaction costs are minimal and decentralized systems do not charge currency conversion fees.
- *Accessibility:* Cryptocurrencies by their very nature are not subject to the exchange rates, interest rates, transactions charges, or other levies imposed by a specific country.
- *Instant Payments are enables by the* peer-to-peer transactions.
- *Improved security provided by Blockchain technology* than the centralized financial systems, which makes it extremely difficult for hackers to infiltrate.
- *Transparency in the transactions.*
- *Decentralization framework in support of* stakeholder governance, putting decision-making powers in the hands of individuals, not central authorities.
- *Immutability:* The immutable nature of the blockchain's general ledger removes the chance for internal actors to manipulate data to their benefit.

4.8 Roadmap for building machine learning systems

In order to improve on Cybersecurity and cyber risk management, a machine learning approach is the best solution as depicted by the roadmap shown on Fig. 11 below.

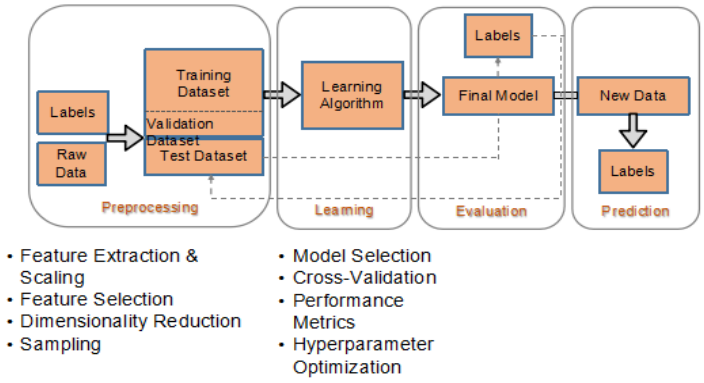


Fig. 11. Roadmap for building machine learning systems.

Machine learning is one of the most exciting recent technologies in Artificial Intelligence. Learning algorithms are now being extensively used in search engines used by Google or Bing. According to [11] the ultimate goal of AI is to develop human like intelligence in machines which can be accomplished through learning algorithms which try to mimic how the human brain learns [10]. Lifelong Machine Learning, or LML, considers systems that can learn many tasks over a lifetime from one or more domains. They efficiently and effectively retain the knowledge they have learned and use that knowledge to more efficiently and effectively learn new tasks.

4.9 The key issues in machine learning worthy of consideration are as follows:

- What algorithms can approximate functions well and when
- How does the number of training examples influence accuracy
- Problem representation / feature extraction
- Intention/independent learning
- Integrating learning with systems
- What are the theoretical limits of learnability?
- Transfer learning
- Continuous learning

4.10 Framework for blockchain technology application and cyber risks

The framework for Blockchain Technology Application Model is closely associated with basic values of communication such as confidentiality, integrity, authenticity, non-repudiation and availability. The key aspects of bitcoins are:

- *Confidentiality;* the system has privacy or ability to control access to bitcoin transactions so only authorized individuals can view sensitive information. Confidentiality is provided by having a public key to assign ownership rights and a private key to certify the transaction. Miners verify the transaction on the blockchain, but anyone on the network can also use the public key to verify the transcation.
- *Integrity;* information of each bitcoin transaction is accurate and reliable and cannot be subtly changed or tampered with by an authorized party. Blockchain records are kept of all transactions.
- *Authenticity;* All the transactions in blockchain are authentic. This is correlated to the ability to verify the content of the bitcoin transaction which cannot be changed in an unauthorized manner.
- *Non-repudiation;* meaning that the origin of any action on the bitcoin system can be verified and associated with a user, with no possible denial. Every miner has their own key and certain record of transaction which comprises a combination of number and letter.
- *Availability;* The information and other critical assets of bitcoin transaction must be accessible to miners and the business when needed [19].

4.11 How does the BT model address cyber risks?

- *No double-spending:* No double-spending means that once a CBDC owned by a user has been transferred, it cannot be used to pay for other transactions. Unlike a physical currency, CBDC, uniquely identified by a sequence of serial numbers, can be copied and saved multiple times. Therefore, no double-spending is the basic security that all digital currencies need to consider.
- *Unforgeability:* Unforgeability requires that no one can falsify CBDCs issued by the Central Bank or forge a CBDC that is not owned by him/her. These forged CBDCs cannot pass verification. CBDC also requires anti-counterfeiting technology to ensure currency security, just like physical currency.
- *Non-repudiation:* Non-repudiation requires that all participants' actions be recorded from the initiation of the transaction to the end, including the payer, the recipient, and the transaction verifier. No one can deny the transaction steps that he has completed.

- *Verifiability:* Verifiability requires that all transaction records involved in the CBDC system can be validated effectively. This is crucial for CBDC as a currency of circulation and a means of payment. It is also the basis for other security properties.
- *Anonymity:* The physical currency is anonymous in actual circulation. Similarly, CBDC should also be designed for user privacy and anonymity. Throughout the development of cryptocurrencies, the anonymity of CBDC mainly includes anonymity of identity and anonymity of transaction. Intuitively, they require that any unauthorized user cannot obtain, calculate, or infer the identity of a user and the information of a transaction through open source data.

5. Conclusion

Blockchain is a significant technological breakthrough in decentralized cryptocurrencies [24] permitting remote peer-to-peer value transfers amongst parties devoid of a trusted third party. The factors that blockchain may affect the development of payment industry and CBDC include:

- Cost: Blockchain-based payment systems may offer lower transaction cost than other payment methods, especially in cross-border payment, currency exchange and other payment scenarios involving multiple intermediary entities.
- Usability: Compared with traditional payment methods, blockchain-based payment methods have some usability advantages, because the blockchain makes the transaction process more intuitive and easier to integrate with other services.
- Anonymity: Although the blockchain itself does not provide any privacy protection; it provides an effective network architecture for anonymous payment. Some blockchain-based cryptocurrency schemes allow users to conduct transactions without providing their own real credentials.

6. Benefits of Block-chain Technology to the Financial Services Sector

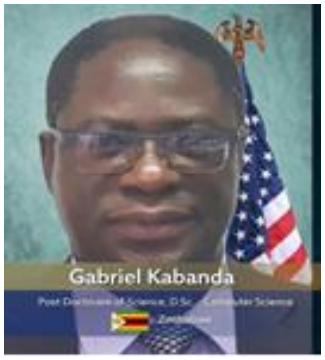
Below is the summary of the ways in which block-chain technology and cryptocurrency benefits the Financial Services sector:

- Costs Reduction
- Faster Transactions
- Improved Security [14].
- Improved Data Quality
- Digital Currencies
- Accountability
- Compliance
- Reduced Error Handling & Reconciliation
- Increased Transparency
- Ease of Money Transfers
- Reduced Fraud Via Self Sovereign Identity

REFERENCES

1. Abdelwahed IM, Ramadan N, and Hefny HA. Cybersecurity Risks of Blockchain Technology. Int J Comput Appl. 2020;177:42.
2. Alanezi AA. Development of an Orally Disintegrating Mini-Tablet (ODMTs) Containing Metoclopramide HCl to Enhance Patient Compliance. Masteer's thesis, Unive Toledo, 2014. [Online]. Available: http://rave.ohiolink.edu/etdc/view?acc_num=mco1417861431
3. Atlam HF, Walters RJ, and Wills GB. Fog computing and the internet of things: A review. In *Big Data and Cognitive Computing*, 2018. [Online]. Available: https://doi.org/10.3390/bdcc2020010
4. Berman DS, Buczak AL, Chavis JS, et al. A survey of deep learning methods for cyber security. Information. 2019;10:122. [Online]. Available: https://doi.org/10.3390/info10040122
5. Brecese J. Research Note Money from Nothing: The Socioeconomic Implications of cyber--currencies, 2013.
6. Bringas PB and Santos I. Bayesian Networks for Network Intrusion Detection, Bayesian Network, Ahmed Rebai (Ed.), InTech, 2010. [Online]. Available: http://www.intechopen.com/books/bayesian-network/bayesian-networks-for-network-intrusion-detection.
7. Demir N and Dalkilic G. Modified stacking ensemble approach to detect network intrusion. Turkish J Electric Eng Comput Sci. 2017, to be published.
8. Elmamy SB, Mrabet H, Gharbi H, et al. A survey on the usage of blockchain technology for cyber-threats in the context of industry 4.0. J Sustainab. 2020;12(21):9179.
9. GSMA. Mobile Economy 2018. GSMA Intelligence, 2018.
10. Hall M. Chronic renal disease and antenatal care. In *Best Practice and Research: Clinical Obstetrics and Gynaecology*. 2019. [Online]. Available: https://doi.org/10.1016/j.bpobgyn.2018.10.002
11. Higginbottom K. *Emotional Intelligence Undervalued in The Hiring Process*. Forbes, 2018.
12. Idebdou N. A game of coins: The digitization of money and the regulation of virtual currencies, 2015.
13. Lewis RE, Heckman RJ. Talent management: A critical review. *Human Resource Management Review,* 2016. [Online]. Available: https://doi.org/10.1016/j.hrmr.2006.03.001
14. Mulders PFA. Abstracts voorjaarsvergadering NVU, 16 en 17 mei 2019, Rotterdam. *Tijdschrift Voor Urologie*. 2019. [Online]. Available: https://doi.org/10.1007/s13629-019-0255-6
15. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, 2018.
16. Nielsen R. CS651 computer systems security foundations 3d imagination cyber security management plan, Technical Report, Los Alamos National Laboratory, USA. 2015.
17. Peter GR, Artur P, and Peter HF. A pragmatic research philosophy for applied sport psychology. Ph.D dissertation, Kinesiology, Sport Studies and Physical Education Faculty Publications, 80, 2005. [Online]. Available: https://digitalcommons.brockport.edu/pes_facpub/80
18. Stallings W. Operating System Stability. Accessed: 27th Mar. 2019, 2015. [Online]. Available: https://www.unf.edu/public/cop4610/ree/Notes/PPT/PPT8E/CH15-OS8e.pdf
19. Tampi MM. menakar progresivitas teknologi finansial (fintech) dalam hukum bisnis di indonesia. era hukum - Jurnal Ilmiah Ilmu Hukum. [Online]. Available: https://doi.org/10.24912/erahukum.v16i2.4529

20. Truong TC, Diep Qb, and Zelinka I. Artificial intelligence in the cyber domain: Offense and defense. Symmetry 2020, 12, 410.
21. Schuessler DL. Beyond content: How teachers manage classrooms to facilitate intellectual engagement for disengaged students. Theory Into Practice. 2009;48(2):114-121.
22. Kessler JB and Hunt A. The welfare effects of nudges: A case study of energy use social comparisons. Amer Econ J: Appl Econ. 2019;11(1): 236-276.
23. Danho and Habte. Blockchain for financial inclusion and mobile financial services: A study in sub-Saharan Africa[D]. 2019.
24. Kabanda G. Applied Business Informatics Module Lecture Notes, University of Zimbabwe, 2020.
25. Nowinski W and Kozma M. How can blockchain technology disrupt the existing business models? Entrepreneurial business and economics review, centre for strategic and international entrepreneurship at the Cracow University of Economics. 2017;5(3):173-188.
26. Abdelwahab SAM, Abdellatif WSE, Hamada AM. Comparative analysis of the modified perturb & observe with different MPPT techniques for PV grid connected systems. Int J Renew Energy Res. 2020;10(1):156-164.



Gabriel Kabanda received Postdoctorate of Science and Doctor of Science (D.Sc.) degrees in computer science from Atlantic International University (USA), the Ph.D. degree in computer science from California, PWU, the M.Sc. degree in computer science from Swansea University, United Kingdom, the B.Sc. degree in mathematics and Physics fro the University of Zimbabwe, Gold Diploma in computer programming , London, U.K, a Certificate in Applied Meteorology (Reading, UK), a Certificate in E-Moderationfrom the University of Cape Town and a Certificate in Management of Higher Education Institutions (Galilee International Management Institute, Israel). He is currently a Full Professor of computer science and information systems, and an Adjunct Professor of cybersecurity for both the Cybersecurity for Executives Program Faculty, Regional and Continuing Education, California State University, Chico, USA, and Ithaca College, New York, ZSchool Adjunct Faculty (USA). He has published 84 publications, eight books, six book chapters, eight edited volumes and 61 research papers published in international refereed journals and supervised 11 PhD candidates in Information Technology/ Computer Science/ Information Systems and over 100 Masters dissertations. He has been teaching the MBA Applied Business Informatics course (previously called MIS/BIS) at the University of Zimbabwe since 2000. He is also the Secretary General of the Zimbabwe Academy of Sciences, Secretary General of the Africa-Asia-Dialogue Network, a Fellow of the African Scientific Institute, USA, a member of the African Science, Research and Innovation Council (ASRIC) of the African Union, and a Fellow of the Zimbabwe Academy of Sciences. He is the former Pro Vice Chancellor (Research, Innovation and Enterprise Development) of Zimbabwe Open University where he spent 13 years in Senior Management position with the university.

Citation: Kabanda G. Cybersecurity risk management plan for a blockchain application model. Trans Eng Comput Sci. 2021;2(1):121